FieldComm Group™
Connecting the World of Process Automation

Product Security Advisory

Vulnerability in hipserver

Document ID	fcg.psa.20201006001
Publication Date	6 Oct 2020

1 Affected Products

HART-IP Developer kit, Release 1.0.0.0 (Licensed Product)
hipserver, Release 3.6.1 (initial public release) (https://github.com/FieldCommGroup/hipserver)

2 Identifier

FieldComm Group ID: PSI-20200601001

CVE ID: CVE-2020-16209

3 Severity

9.8 CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

4 Indented Audience

License holders to the HART-IP Developer Kit and users of hipserver open source code.

5 Description

The HART-IP server component hipserver takes HART-IP messages from its clients and transports the embedded HART messages to various HART application programs. An unchecked memory transfer in the IP interface would potentially allow an internal buffer to overflow.

6 IMPACT

A malicious user could exploit this interface by constructing HART-IP messages with payloads sufficiently large to overflow the internal buffer and crashing the device or obtaining control of the device.

7 REMEDIATION

Users of version hipserver v3.6 can protect themselves by restricting access to the computers or devices running the software. Users of hipserver should immediately upgrade their source code to use v3.7.0 (or higher)

All licensed users of the HART-IP developer kit will be sent updated source code.

The hipserver source code was added to the GitHub repository on 5 Dec 2019. As of this advisory notice, FieldComm Group is not aware of any third-party commercial products using hipserver.

8 CREDIT

The researcher Reid Wightman from Dragos, Inc identified the security vulnerability.

Advisories and Disclosure coordinated through CISA.

9 CONTACT INFORMATION

For technical support, please visit https://support.fieldcommgroup and file a support ticket. You can also directly contact FieldComm Group by visiting https://fieldcommgroup.org

10 REVISION HISTORY

6 Oct 2020 1.0 Initial Version (this document)

11 TERMS OF USE

Original versions of this document are available at https://fieldcommgroup.org